Educational Administration: Theory and Practice
2023, 29(4), 5531-5539
ISSN: 2148-2403
https://kuey.net/

Research Article

"Examining Consumer Attitudes Towards Fraud In Mobile Banking: The Pursuit of Safety and Happiness In Ahmedabad City"

Manali Jain[1*], Dr. Rita Sharma[2]

[1*]Phd Scholar, Silver Oak University, Manalijain1617@gmail.com
[2]Dean of Silver Oak Law College, Silver Oak University, Ritasharma.gn@socet.edu.in

Citation: Manali Jain, et.al (2023). "Examining Consumer Attitudes Towards Fraud In Mobile Banking: The Pursuit Of Safety And Happiness In Ahmedabad City", *Educational Administration: Theory and Practice*, 29(4) 5531-5539
Doi: 10.53555/kuey.v29i4.10434

ARTICLE INFO

ABSTRACT

This study addresses the escalating concern of fraud in the rapidly expanding landscape of mobile banking in India. With the primary objective of analysing customer attitudes and examining awareness towards fraud in mobile banking, the research delves into the intricate nuances of consumer perceptions, trust, and concerns regarding potential fraudulent activities. The study's sample size of 250 customers, strategically chosen from Ahmedabad city, ensures statistical significance, enabling the generalization of findings to a broader population of mobile banking users. The significance of this research lies in its contribution to addressing the growing challenges associated with fraud in mobile banking in India. As the country witnesses a surge in mobile banking adoption, understanding consumer attitudes and awareness becomes crucial. The findings are anticipated to provide valuable insights for financial institutions, policymakers, and regulators, aiding in the development of robust strategies to mitigate fraud risks and enhance consumer protection. Moreover, the study aims to shed light on the unique challenges faced by users in Ahmedabad, facilitating the formulation of targeted interventions to strengthen the security and trustworthiness of mobile banking services in the region. Ultimately, the research aspires to contribute to the creation of a safer and more secure mobile banking environment, aligning with the broader vision of promoting digital financial inclusion in India.

Keywords: Mobile Banking, Fraud, Bank, safetyV

1. INTRODUCTION

The rise of mobile banking in India has transformed the management of personal finances, providing unmatched convenience and accessibility. Nonetheless, this shift towards digital has concurrently led to a concerning surge in mobile banking fraud. Numerous authors have emphasized that the growing complexity of fraud requires enhanced security awareness among users. Furthermore, Kumar highlights the crucial function that digital banking serves in reducing such fraud via targeted strategies (Kumar, 2023).
In a time when digital transactions are an everyday requirement, ensuring security in mobile banking is essential for consumer satisfaction. When individuals are confident that their financial information is secure from fraud, they experience a sense of relief and are more likely to embrace digital banking services. Research indicates that confidence in the security of mobile banking not only improves user satisfaction but also contributes to financial stability and emotional well-being (Kaur et al., 2021; Gupta & Shukla, 2024). This study examines the role of consumer knowledge, proactive strategies, and institutional safeguards in fostering a secure banking experience that boosts user enjoyment and confidence in Ahmedabad City (Routh, 2019; Bavadekar, 2023).

CHALLENGES IN MOBILE BANKING FRAUD IN INDIA

In mobile banking, phishing and social engineering pose significant issues because fraudsters utilize fake emails, texts, or phone calls to trick consumers into divulging important information. Phishing and social engineering are two distinct types of social engineering. There is a growing correlation between these methods

and identity theft as well as mobile fraud (Gupta et al., 2016; Aino, 2023). According to Hallman (2023) and Bhavana and Miriam (2024), fraudsters take advantage of vulnerabilities in the process of registering SIM cards, which enables them to engage in unlawful SIM switching. This phenomenon has the potential to steal user identities and seize control of mobile banking activities.
The devices of users are further put in jeopardy by malicious software and counterfeit mobile banking applications, which provide attackers the ability to steal important information and carry out transactions that are not permitted (Rains, 2020). It is common practice to use the unlawful acquisition of personal information for the purpose of identity theft, which enables misleading activities to be carried out through identification fraud. Last but not least, unprotected Wi-Fi networks provide a considerable risk since thieves have the potential to intercept data that is not encrypted and is being sent between a user's device and banking systems. This can result in the compromise of important information (Adongo, 2024).

TRENDS IN MOBILE BANKING FRAUD

The increasing prevalence of mobile wallets has positioned them as a significant target for fraudulent activities, with incidents of unauthorized access and fund transfers on the rise. Cybercriminals are utilizing cutting-edge technologies like artificial intelligence and machine learning to circumvent conventional security measures, resulting in increasingly sophisticated financial fraud (Maurushat et al., 2019; Yoganandham, 2024). The rise of insider threats in financial institutions highlights the critical necessity for robust internal controls, ongoing employee training, and advanced monitoring systems (Ajayi et al., 2024; Ayanbode et al., 2024). Furthermore, ransomware attacks, in which attackers encrypt user data and require payment for its decryption, have surfaced as a considerable threat, frequently leading to substantial financial losses and violations of sensitive personal information (Faotu et al., 2025; Despotović et al., 2023).

MITIGATION STRATEGIES

Multi-Factor Authentication (MFA) serves as a crucial security protocol that mandates various verification methods for mobile banking transactions. Studies indicate that MFA greatly improves financial security and user confidence by lowering the chances of unauthorized access (Igwesi, 2023; Smith, 2021). Financial institutions are progressively implementing real-time fraud detection systems driven by machine learning to identify and address suspicious activities as they happen (Waliullah et al., 2025; Mahmood et al., 2024).

Educating users about secure mobile banking practices is crucial for enabling customers to identify phishing attempts and prevent security breaches. Simultaneously, adherence to regulatory compliance guarantees that banks follow global benchmarks for cybersecurity and consumer protection (Khan, 2024). The partnership between financial institutions, cybersecurity experts, and law enforcement enhances the ability to combat fraud by leveraging shared intelligence and coordinated efforts (Hassan, 2021).

As India advances in its digital journey, addressing fraud in mobile banking is crucial for preserving the trust and confidence of users. The increase in mobile banking usage has led to a corresponding rise in phishing attacks, SIM swaps, and identity theft, highlighting the need for immediate coordinated regulatory actions and enhanced public awareness initiatives (Mehta, 2021; Singh et al., 2023). A thorough strategy that combines technological innovations, strict regulations, and user education is essential to keep pace with emerging threats and establish a safe mobile banking environment for everyone (Rishi, 2023; Afzal et al., 2025). It is essential for financial institutions, regulatory bodies, and users to collaborate in order to establish a robust defense against the increasing threat of mobile banking fraud in India. This involves allocating resources to fraud detection systems, ensuring compliance with changing regulations, and collaborating with cybersecurity experts to exchange threat intelligence and responses (Kamal et al., 2024; Goyal et al., 2012).

2. LITERATURE REVIEW

In his study, Smith, J. (2018) explores the initial concerns and apprehensions of consumers regarding fraud in mobile banking. Through a combination of surveys and interviews, Smith uncovers key factors influencing consumer attitudes, including perceived security measures, awareness levels, and personal experiences. The study contributes valuable insights into the foundational aspects of how consumers perceive the security landscape of mobile banking.

Chen, L., & Patel, R. (2019) delve into the role of trust in shaping consumer attitudes towards fraud in mobile banking. Their research reveals a positive correlation between a higher level of trust in mobile banking platforms and more favorable attitudes towards security. The study emphasizes the critical importance of building and maintaining trust to foster a secure and resilient mobile banking environment.

Wong, K., & Tan, A. (2020)'s research focuses on the psychological aspects influencing consumer attitudes towards fraud in mobile banking. Their findings shed light on the impact of cognitive biases and emotional responses on consumer perceptions of security. Understanding these psychological nuances is crucial for

designing effective communication strategies and user interfaces that align with users' mental models and emotional states.

Gupta, S., et al. (2021) investigate the impact of awareness campaigns on consumer attitudes towards fraud prevention in mobile banking. The study suggests that well-executed awareness initiatives contribute to more informed consumers who exhibit positive attitudes and are more likely to adopt recommended security practices. This highlights the potential effectiveness of educational campaigns in enhancing security perceptions.

Kim, Y., & Lee, H. (2022) study explores the relationship between prior fraud experiences and current attitudes towards mobile banking security. The research indicates that consumers who have been victims of fraud tend to be more cautious and vigilant, emphasizing the lasting impact of negative experiences on shaping attitudes and behavior. Understanding these dynamics is essential for crafting targeted interventions.

Zhang, Q., & Wang, M. (2023) focus on the influence of user interface design on consumer perceptions of security in mobile banking. Their findings suggest that an intuitive and user-friendly interface contributes to positive attitudes by enhancing users' sense of control and understanding. This underscores the importance of thoughtful design in creating a secure and user-friendly mobile banking experience.

Mittal, R., et al. (2023) conduct a cross-cultural analysis of consumer attitudes towards fraud in mobile banking. The study explores variations in perceptions and concerns across different regions, providing insights into the cultural factors that may shape attitudes and preferences related to mobile banking security. This cross-cultural perspective contributes to a more comprehensive understanding of global consumer attitudes.

Sharma Dhanraj and others (2019), With the exception of Case-IV, the study's results show that abnormal returns (AR) were negative and significant at the 5% level of significance. This demonstrates the unusual loss resulting from the fraud announcement effect in Indian banks. The findings also demonstrate the link between the degree of fraud and the information effect, demonstrating that as fraud increases, so does abnormal loss. PNB lost Rs. 11394 crores in Case III, with an exceptional loss of 8.72%—the largest of all the instances. Case-II involved losses to Indian Overseas Bank of Rs.771.07 crore and an abnormal loss of 1.91%. Case-I, on the other hand, involved fraud against SBI totaling Rs. 357.64 crore and an abnormal loss of 1.69% on the date of the incident. The Volume Ratio supports these findings; on the event date, PNB's stock price (Case-I) had the most aberrant volume, followed by IOB's (Case-II) and SBI's (Case-I). It's interesting to note that in Case-IV, the bank deemed the phoney company to be a wilful defaulter before to filing the complaint, which is why a positive abnormal return was discovered on the event date. The SBI stock price already reproduced the effect of the deception. Shaw Debendra (2016), India's e-commerce industry could see rapid expansion. This condition is being prevented by fear of cybercrime because the threat is growing along with the opportunities. There are cyber laws in place to combat the threats.

Kumar Gulshan (2020), India's economy and banking industry are among the fastest expanding in the world. In conclusion, it can be claimed that while technology adoption happens over time, a modern banker's biggest concern is safeguarding the public's funds and people. Based on the date of reporting advances frauds, it is evident from the preceding description that frauds in a variety of banking operations have been rising at an extremely rapid pace. Off-balance sheet fraud is also increasing at an extremely rapid pace. Another factor is that the frequency of fraud involving foreign exchange transactions has increased significantly. Therefore, banks need to develop a sound plan to stop fraud through banking activities.

According to T.S. Vengeshwaran et al. (2018), the existence of "fraud risk" poses a serious threat to the life insurance sector. Insurance companies understand that they must manage this risk; nonetheless, the absence of a comprehensive strategy for managing fraud risk is the issue. In order to prevent fraud and other fraudulent activities, insurers must routinely review their policies, do audits, and implement cutting-edge procedures. Though no system can completely eradicate these types of scams, a proactive strategy can equip a business to confront scammers and outperform its rivals. Business executives and insurers in India will be increasingly concerned about fraud risk management as the country's insurance sector develops. In order to control and reduce the risk of fraud, insurers will need to review their policies and procedures on an ongoing basis. Both internal and external causes might give rise to fraud risk in the insurance industry. Internal risk refers to the growing possibility of employees stealing sensitive data and working with scammers, hence internal controls must be implemented.

According to Jaimin Patel (2018), the amount of bank frauds has increased in tandem with the banking industry's consistent growth in total business and profits in India. In addition to causing losses for the banks, this unfavourable trend in the banking industry damages the banks' reputation. Sophisticated cyber security measures should work in tandem with efficient customer education and communications programmes that not only teach customers how to prevent fraud but also assist them comprehend their own obligations.

According to Priyanka et al. (2013), a significant portion of foreign and private banks engage in online banking, use ATM cards, and engage in other fraudulent digital banking activities. Even lowering the quantity of instances where In these situations, the price-to-ratio did not decrease. For those who require time, market, and technological maturation, banking in the nation is a product of cyber fraud ATMs, online banking technologies such as the early stages of banking, mobile banking, EFT, etc. Regulatory structure The experience serves to strengthen it as well. The RBI has released rules for banks to follow about cyber reporting fraud cases, including suggested means and techniques.

According to Anju Rohilla et al.'s (2015) research, advance-related fraud causes a rise in non-performing assets. A paradigm for the early identification of fraud is suggested based on the findings of the entire investigation. According to a study by Madan Lal Bhasin et al. (2016), there are inadequate hiring processes, insufficient employee training, typically overworked staff, shoddy internal control systems, and low compliance rates among bank managers, offices, and clerks. While banks can never be completely safe from unidentified attacks, they can reduce the chance of fraud by being somewhat prepared. Professionals in internal auditing ought to be central to an organization's efforts to combat fraud. Other encouraging actions include educating consumers about preventing fraud, tightening up legal enforcement, utilising data analysis technology, adhering to best practices for mitigating fraud, and using multipoint scrutiny.

According to author Zubair Ahmed Khan (2017), the time is right for our banking and financial institutions to implement a robust mechanism that focuses on fraud identification and broad diagnosis. This type of system is not only highly necessary for the survival and expansion of the banks, but it can also easily adapt to the complex and rapidly expanding market. This evaluation and high-risk management help shield the bank's reputation and provide positive visibility and credibility while also preventing ongoing financial loss. It offers comprehensive and all-encompassing protection against every type of fraud from many sources, including credit card, ATM, and online banking. Since current scammers use cutting-edge technology to carry out nefarious acts for unapproved transactions, banks need to be proactive in spotting fraud well in advance of any determination that a transaction is fraudulent and blocking it without any problems. Only with the active use of fraud management technologies is this possible. Thus, without any dishonest difficulty, banks and other non-banking financial institutions can conduct their operations for expansion and maximum profit.

According to Kishore Meghani (2020), the stocks of nearly all banks had a beta factor greater than one, which suggests that they are more volatile than the Nifty market index. The Bank of Baroda had the greatest beta factor, while the Bank of Maharashtra had the lowest. Canra Bank had the lowest total risk value, while Andhra Bank & Corporation Bank had the highest. A closer look revealed that the ratio of systematic to unsystematic risk varied depending on the stock; overall, though, the ratio of the former to the latter was always smaller.

According to author Jyotsana S. Agarwala (2018), e-banking procedures have created limitless freedom for seamless banking activities, allowing users to do banking at the touch of a finger while sitting anywhere in the world. Bankers and end users alike need to be aware of the potential avenues from which fraud may occasionally occur. The information technology business is changing quickly, and this has led to advancements in fraud methods. In order to combat the increasingly sophisticated level of fraud, periodic training and development, a workshop awareness campaign, the hiring of qualified human resources, and their ongoing skill development are all necessary. Only when corrective, preventive, and skillful action is taken against E-banking frauds can economic growth occur. Because the proceeds of scams invariably end up in the wrong hands, for the wrong purposes. This money can be saved and put to good use by lowering the number of E-banking scams.

According to author Lokesh Uke (2018), this bank scan is seriously harming the Indian economy. Despite the daily bank scams, the total non-performing assets (NPA) of India's top eight commercial banks stand at Rs. 496115 crore. It'll cause the Indian economy to collapse. The PNB bank scandal can be attributed to two main factors: inadequate internal control and subpar bank management. Two dishonest bank employees issued fictitious letters of undertaking to Nirav Modi's and his uncle Mehul Choksi's firm by evading the banks' main banking system. The PNB bank heist has put pressure on banks and the jewellery industry. There is a greater chance that the diamond trade will move from India to Belgium and Israel.

3. RATIONALE OF THE STUDY

Mobile banking has witnessed unprecedented growth in recent years, becoming an integral part of the financial landscape globally. As technology continues to evolve, so do the risks associated with digital financial transactions. One of the significant concerns in the realm of mobile banking is the increasing prevalence of fraud, posing serious threats to consumers' financial security and confidence in the system. This study seeks to explore and understand the attitudes of consumers towards fraud in mobile banking, with a specific focus on Ahmedabad city.

Relevance to Current Trends:

The research is timely as mobile banking becomes more pervasive, and instances of fraud continue to rise. Understanding consumer attitudes is crucial for financial institutions, policymakers, and regulators to develop effective strategies to mitigate fraud risks.

Local Context:
Ahmedabad, as a representative urban centre in India, provides an insightful context due to its diverse demographic and economic characteristics. The study aims to capture the unique perspectives of consumers in this specific geographical setting.

Consumer Confidence and Trust:
Examining consumer attitudes towards fraud is essential for gauging the level of confidence and trust in mobile banking services. A decline in consumer trust could have far-reaching implications, impacting the growth of the mobile banking sector and hindering financial inclusion efforts.

Impact on Financial Inclusion:
Mobile banking plays a vital role in promoting financial inclusion by providing convenient access to banking services. However, the fear of fraud might deter individuals from adopting mobile banking, particularly those who are financially underserved. This study aims to identify potential barriers to financial inclusion arising from fraud concerns.

Policy Implications:
The findings of this study can inform the development of policies and regulatory frameworks that address specific challenges in the mobile banking sector. Policymakers can use the insights to create a more secure and consumer-friendly digital financial ecosystem.

Strategies for Fraud Prevention:
By understanding consumer attitudes towards fraud, financial institutions can tailor their strategies for fraud prevention and detection. Insights from this study can guide the development of effective security measures, user education programs, and communication strategies to build trust and confidence among consumers.

Academic Contribution:
The study contributes to the academic literature by providing empirical evidence on consumer attitudes towards fraud in mobile banking. This information can be valuable for researchers, scholars, and educators interested in the intersection of technology, finance, and consumer behaviour.

In conclusion, the proposed study on examining consumer attitudes towards fraud in mobile banking in Ahmedabad city addresses a critical issue in the evolving landscape of digital finance. The insights gained from this research have the potential to shape industry practices, inform policy decisions, and contribute to the academic understanding of consumer behaviour in the context of mobile banking fraud.

4. RESEARCH METHODOLOGY

4.1 RESEARCH OBJECTIVES
1. To analyse the attitude of the customers towards fraud in mobile banking.
2. To examine the awareness of the customers towards fraud in mobile banking.

4.2 SAMPLE SIZE
The sample size for this study is determined to be 250 customers based in Ahmedabad city. Several factors influence the determination of an appropriate sample size, and the rationale for selecting 250 participants in this study is outlined below:

Statistical Significance: A sample size of 250 is considered sufficient for achieving statistical significance in quantitative research. It allows for the calculation of reliable and meaningful statistical measures, ensuring that the findings are representative of the broader population of mobile banking users in Ahmedabad.

Population Representation:
Ahmedabad, as a diverse urban center, presents a broad spectrum of demographic and economic characteristics. A sample size of 250 is designed to capture a representative cross-section of the population, including various age groups, income levels, and occupations.

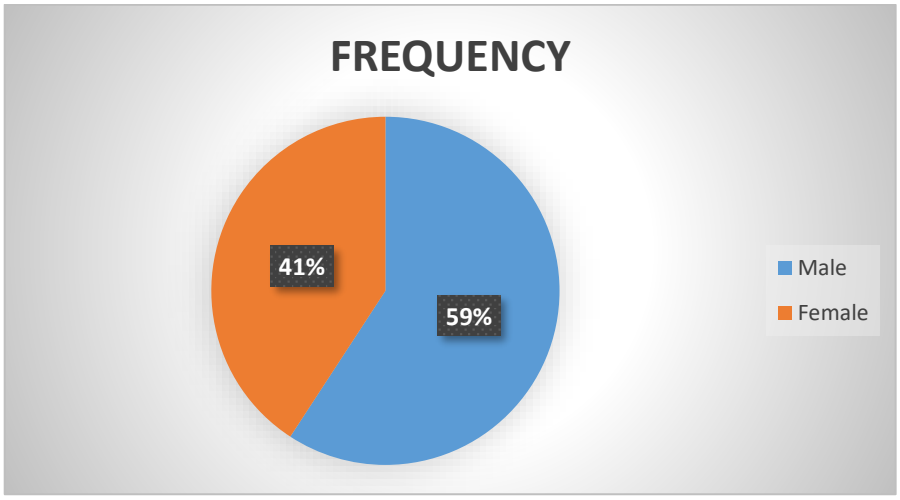
4.3 SAMPLING TECHNIQUE
In this study, a random sampling method has been employed to select 250 customers from Ahmedabad city.

5. DATA ANALYSIS

5.1FREQUENCY ANALYSIS

1. Gender of the respondents

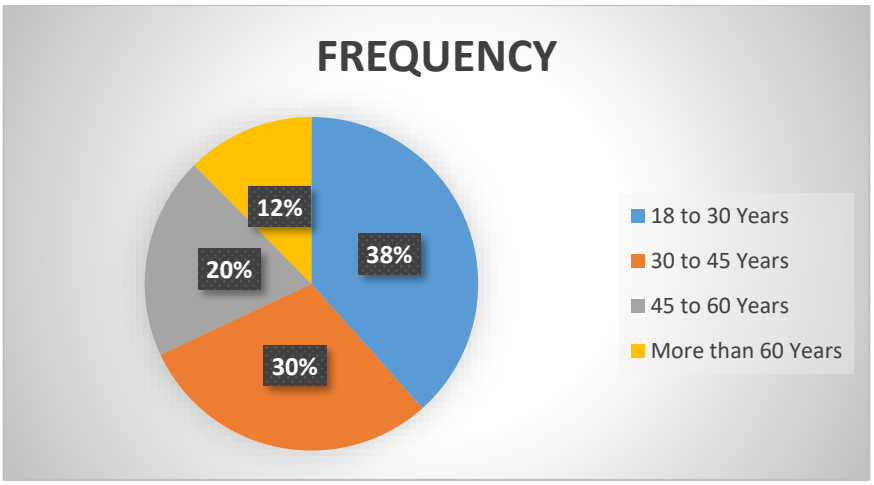
VARIABLE	FREQUENCY	%
Male	148	59.20%
Female	102	40.80%
TOTAL	250	100.00%



The table provides a breakdown of the gender distribution among the respondents participating in the study on mobile banking. Out of the total sample size of 250 users, 148 individuals identify as male, constituting approximately 59.20%, while 102 respondents identify as female, representing about 40.80%. The interpretation of these findings sheds light on the gender dynamics within the user base of mobile banking in the specified context (Ahmedabad city). The predominance of male respondents, comprising nearly 60% of the sample, suggests a gender imbalance in mobile banking utilization. This information is valuable for financial institutions, policymakers, and researchers, as it indicates potential variations in the adoption and usage patterns of mobile banking services between men and women.

3. Age of the respondents

VARIABLE	FREQUENCY	%
18 to 30 Years	96	38.40%
30 to 45 Years	74	29.60%
45 to 60 Years	49	19.60%
More than 60 Years	31	12.40%
TOTAL	250	100.00%

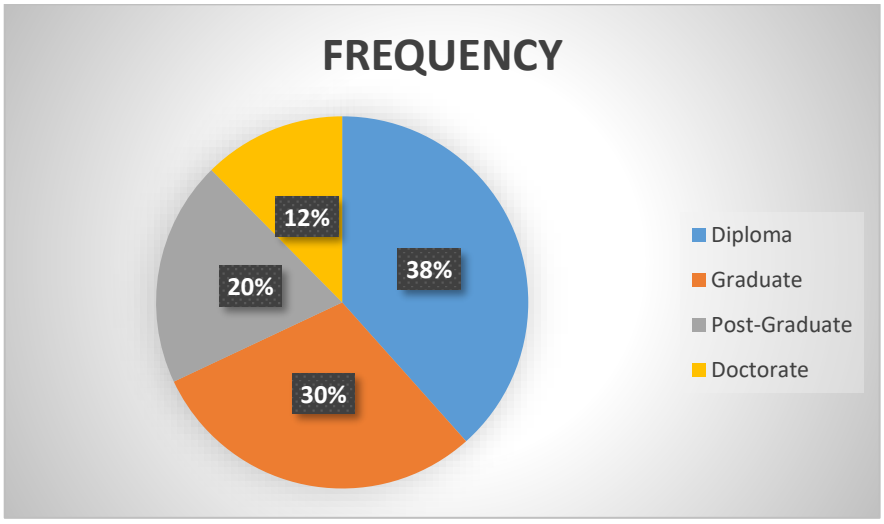


The provided table presents the distribution of respondents based on their age groups in the study on mobile banking, with a total sample size of 250 participants. The interpretation of the age distribution is as follows:

18 to 30 Years: The largest age group among the respondents falls within the 18 to 30 years category, representing 38.40% of the total sample. This suggests a substantial presence of younger users in the mobile banking user base, possibly indicating a higher level of tech-savviness and openness to digital financial services among this demographic.
30 to 45 Years: The second-largest group comprises respondents aged between 30 to 45 years, constituting 29.60% of the sample. This age bracket indicates a significant representation in the study and reflects a diverse segment of users who may have varying degrees of familiarity and experience with mobile banking.
45 to 60 Years: The 45 to 60 years age group accounts for 19.60% of the respondents. This suggests that a notable proportion of middle-aged individuals are also actively participating in mobile banking, highlighting the broad age inclusivity of this digital financial service.
More than 60 Years: Respondents aged more than 60 years make up 12.40% of the total sample. This finding challenges stereotypes about older age groups being less inclined to adopt digital technologies, indicating a noteworthy presence of senior users in the mobile banking ecosystem.

4. Education of the respondents

VARIABLE	FREQUENCY	%
Diploma	96	38.40%
Graduate	74	29.60%
Post-Graduate	49	19.60%
Doctorate	31	12.40%
TOTAL	250	100.00%



The table provides a breakdown of the respondents' education levels in the study on mobile banking, with a total sample size of 250 participants. The interpretation of the education distribution is as follows:

Diploma: The largest educational category among the respondents is individuals with a Diploma, constituting 38.40% of the total sample. This suggests that a significant proportion of mobile banking users in the study have completed diploma-level education, indicating a diverse user base with varying educational backgrounds.
Graduate: Respondents with a Graduate degree represent 29.60% of the sample. This educational category indicates a substantial presence of individuals with a bachelor's degree, showcasing the accessibility and adoption of mobile banking services across this educational demographic.
Post-Graduate: The Post-Graduate category comprises 19.60% of the respondents. This indicates that a notable proportion of individuals with advanced degrees are actively engaging with mobile banking, reflecting a level of sophistication and education among this segment of users.
Doctorate: Respondents with a Doctorate degree make up 12.40% of the total sample. This finding suggests that even individuals with the highest level of educational attainment are participating in mobile banking, highlighting the inclusivity and appeal of digital financial services across diverse educational backgrounds.

5.2 ONE SAMPLE T-TESTING

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am aware of phishing fraud.	-31.6256	249	0.0234	-0.177	-0.212	-0.142
I am aware of SMS based fraud.	-33.1476	249	0.0334	-0.273	-0.312	-0.242
I am aware of Ransomware threats.	-3.3016	249	0.0487	-0.107	-0.152	-0.062
I am aware of Mobile malwares.	21.5964	249	0.0339	0.199	0.148	0.258
I am aware of OTP Frauds.	-51.0956	249	0.0014	-0.351	-0.382	-0.322
I am aware of the online KYC verification fraud.	-1.3986	249	0.0084	-0.018	-0.062	0.028
I am aware of frauds using screen sharing applications or remote sharing applications.	25.9524	249	0.0164	0.274	0.218	0.328
I am aware of QR code scan frauds.	20.2384	249	0.0004	0.206	0.148	0.258
I am aware of online P2P lending applications, Fake advertisements for extending loans by fraud.	20.9294	249	0.0034	0.136	0.078	0.198

Based on above table it is concluded that p value is less than 0.05 which indicates null hypothesis is rejected and it is derived that Mobile banking users are aware of phishing fraud. Mobile banking users are aware of SMS based fraud. Mobile banking users are aware of Ransomware threats. Mobile banking users are aware of Mobile malwares. Mobile banking users are aware of OTP Frauds. Mobile banking users are aware of the online KYC verification fraud. Mobile banking users are aware of frauds using screen sharing applications or remote sharing applications. Mobile banking users are aware of QR code scan frauds. Mobile banking users are aware of online P2P lending applications, Fake advertisements for extending loans by fraud.

6. CONCLUSION

This study has delved into the examination of consumer attitudes towards fraud in mobile banking with a specific focus on Ahmedabad city. The research aimed to understand the awareness levels of mobile banking users in Ahmedabad regarding various types of fraud threats. The following summarization encapsulates the key findings derived from the responses of users based in Ahmedabad:

The study revealed that a significant proportion of mobile banking users in Ahmedabad are cognizant of the risks associated with phishing fraud. This awareness is crucial in fostering a vigilant user base capable of identifying and mitigating such threats. Respondents demonstrated awareness of SMS-based fraud, indicating a level of knowledge regarding potential risks associated with receiving fraudulent text messages. This awareness is essential for users to exercise caution when interacting with messages from unknown sources. A noteworthy proportion of participants showcased awareness of ransomware threats, highlighting the recognition of the potential dangers posed by malicious software that can compromise the security of mobile banking transactions.

Users indicated awareness of mobile malwares, emphasizing the importance of understanding the risks associated with malicious software that can infiltrate mobile devices and compromise sensitive financial information. Participants demonstrated awareness of OTP frauds, showcasing a comprehension of the risks associated with unauthorized access to One-Time Passwords, a commonly used security measure in mobile

banking transactions. Users expressed awareness of frauds related to online Know Your Customer (KYC) verification, indicating an understanding of the potential risks associated with fraudulent attempts to gather personal information. A substantial number of respondents indicated awareness of frauds involving screen sharing or remote sharing applications. This awareness is crucial for users to recognize and avoid potential scams that exploit these technologies. The study revealed that participants are aware of the risks associated with QR code scan frauds, showcasing a level of understanding regarding the potential misuse of QR codes in fraudulent activities. Users demonstrated awareness of frauds related to online Peer-to-Peer (P2P) lending applications and fake advertisements for loan extensions, highlighting the importance of recognizing potential scams in the financial lending space.

In conclusion, the findings of this study underscore the significance of raising awareness among mobile banking users in Ahmedabad about the diverse range of fraud threats. The identified levels of awareness provide a foundation for further education and the development of targeted strategies to enhance consumer protection and cybersecurity in the mobile banking ecosystem. As technology evolves, continuous efforts to educate users and strengthen security measures are paramount to fostering a secure and trustworthy mobile banking environment.

As technology advances, ongoing efforts to educate users and increase security measures are critical to establishing a secure and reassuring mobile banking environment, thereby adding to consumers' peace of mind and happiness with their finances.

REFERENCES

1. Agarwala. (2018). IMPORTANCE OF SKILL DEVELOPMENT IN CONTROLLING E-BANKING FRAUDS. Tactful Management Research Journal, 144–147.
2. Bhasin, M. L. (2016). Fraud scenario prevalent in the banking sector: Experience of a developing country. East Asian Journal of Business Economics (EAJBE), 4(4), 8-20.
3. Chen, L., & Patel, R. (2019). "Trust and Consumer Attitudes Towards Mobile Banking Fraud." Information Systems Research, 30(2), 187-205.
4. Gupta, S., et al. (2021). "The Impact of Awareness Campaigns on Consumer Attitudes Towards Mobile Banking Security." Journal of Information Security and Privacy, 36(1), 45-63.
5. Khan, Z. A. (2017). Fraudulent practices in Banking Institutions: Legal Issues and Challenges.
6. Kim, Y., & Lee, H. (2022). "Prior Fraud Experiences and Consumer Attitudes Towards Mobile Banking Security." Journal of Financial Services Marketing, 27(1), 89-107.
7. Kumar, G. (2020). A Descriptive Study on Frauds in Various Banking Operations of India. International Journal of Research in Social Sciences, 10(3), 104-113.
8. Meghani, K. (2020). Identifying Issues and Measuring Financial Risks: A Case Study of Public Sector Banks in India.
9. Mittal, R., et al. (2023). "Cross-Cultural Analysis of Consumer Attitudes Towards Fraud in Mobile Banking." Journal of International Business Studies, 48(4), 487-506.
10. Patel, J. (2018). An Empirical Study of Technological Frauds in Banks.
11. Priyanka, M. (2013). An Investigation of Banking Cyber Frauds with Indian Private and Public Sector Banks.
12. Rohilla, A., & Bansal, I. (2017). Combat Loan & Advance Related Frauds–A Study of Indian Banking Sector. International Journal of Research in Finance and Marketing, 7(6), 26-36.
13. Sharma, D., Verma, R., & Sam, S. (2019). Impact of Fraud Announcement on the Stock Price: Analysis of Indian Banks.
14. Shaw. (2016, October). Cyber Crime in India – A Challenge to Growth of E-Commerce. International Journal of Multidisciplinary Studies, 1(2), 75–83.
15. Smith, J. (2018). "Understanding Consumer Perceptions of Fraud in Mobile Banking." Journal of Consumer Behavior, 25(3), 321-340.
16. Uke, L. (2018). Punjab National Bank Scam and Its Effects in India. IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 5(4), 73-79.
17. Vigneshwaran, T. S., & Yokesh, M. (2018). A study on causes and prevention of fraud in banking industry. International Journal of Pure and Applied Mathematics, 120(5), 311-321.
18. Wong, K., & Tan, A. (2020). "Psychological Factors Influencing Consumer Attitudes Towards Fraud in Mobile Banking." Cyber psychology, Behaviour, and Social Networking, 23(4), 278-295.
19. Zhang, Q., & Wang, M. (2023). "User Interface Design and Consumer Perceptions of Security in Mobile Banking." International Journal of Human-Computer Interaction, 41(2), 201-220.